Priority
Send
Enter
Closed
JS-5/JS-6
JS-2/JS-3
Scan Only

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

MYSPACE, INC.,

Plaintiff,

v.

SANFORD WALLACE D/B/A FREEVEGASCLUBS.COM, REALVEGAS-SINS.COM, FEEBLEMINDED PRODUCTIONS,

Defendant.

CV 07-1929 ABC (AGRx)

ORDER GRANTING IN PART PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

On June 11, 2007, Plaintiff MySpace, Inc. ("Plaintiff") filed the instant motion for a preliminary injunction. Defendant Sanford Wallace d/b/a freevegasclubs.com, realvegas-sins.com, and Feebleminded Productions ("Defendant") opposed on June 20, 2007, and Plaintiff replied on June 27, 2007. The hearing on this matter was held on July 2, 2007. Based on the arguments of the parties and the pleadings in this case, the Court hereby GRANTS IN PART Plaintiff's motion for a preliminary injunction.

53

I. STATEMENT OF FACTS

Plaintiff is a "social networking service" that allows members to create unique personal profiles online to find and communicate with other people. (Declaration of Sarah Kaleel ("Kaleel Decl.") ¶ 3.) Plaintiff provides its members with access to the MySpace.com website and the MySpace.com instant messenger and to other Internet-based features, content, and applications offered by Plaintiff in connection with the MySpace.com website. (Id.) Users also have the ability to send and receive communications to and from other MySpace.com users, create groups, and post comments on bulletins. (Id.) To become a member of MySpace.com, a user must create a profile by inputting his or her name, country, zip code, birth date, and gender, must create a password, and must provide an alternate email address to which confirmations and notifications can be sent. (Id. ¶ 4.) Moreover, when registering a user must agree with the Terms of Use Contract (the "TOU Contract") by clicking an "I accept" button and inputting a verification code, a unique series of letters and numbers designed to prevent the use of automated processes to create profiles. (Id.) To access a profile and message inbox, a user must log onto MySpace.com or log on to his or her individual MySpace.com page via an individual Uniform Resource Locator ("URL"). (Id.)

Plaintiff has expended significant time and resources in implementing various measures to prevent abuse of its service and curtail commercial spam (mass mailing of unsolicited commercial email), including limiting the number of messages that can be sent from a single MySpace.com account in a single day and using sophisticated algorithms to identify potential spammers. (Id. ¶ 12.)

Limiting spam is important because it clogs networks, uses up bandwidth, and degrades the user experience. (Id. ¶ 11.)

Plaintiff claims that Defendant has engaged in an abusive multi-faceted scheme to disseminate commercial messages and solicitation to MySpace.com users. Defendant admits that he maintains two websites, freevegasclubs.com and real-vegas-sins.com (the "Wallace Websites"). (Declaration of Sanford Wallace ("Wallance Decl.") ¶ 3.) In October 2006, Plaintiff's abuse team began receiving complaints related to the Wallace Websites and after investigating, it discovered that Defendant had created more than 11,000 similar MySpace profiles and 11,383 unique America Online email accounts to register those profiles. (Kaleel Decl. ¶¶ 16-17.) Because an individual could not easily create this number of unique profiles and because the naming conventions used to create each profile and email address were consistent, the abuse team concluded that Defendant must have used an automated "bot" to register these profiles and addresses. (Id. ¶ 18.)[1] The abuse team concluded that, by creating more than 11,000 unique email addresses, Defendant circumvented Plaintiff's unique-email-address registration requirement and by creating 11,000 unique profiles, Defendant circumvented Plaintiff's daily limit on the number of messages that can be sent from any one profile in a single day. (Id. ¶ 19.)

Plaintiff accuses Defendant of first sending out a series of messages, comments, and bulletins to MySpace users designed to

---

[1]For example, 2,077 of Defendant's MySpace profiles were named "What Pic Should I Upload?" and Defendant's AOL email addresses all consisted of a 10- or 11-digit number followed by "@aol.com." (Kaleel Decl. ¶¶ 16-17.)

redirect users to a website containing a MySpace.com logo and soliciting the member's MySpace.com username and password through a box that closely resembled the box used by members when logging onto MySpace.com. (Declaration of Rick Frazier ("Frazier Decl.") ¶¶ 5-6.) Defendant used this technique (called "phishing") to "hijack" members' usernames and passwords so he could then log onto those other members' MySpace.com profiles and send messages to those users' "friends," directing them to the Wallace Websites. (Id. ¶ 7.) In total, Defendant sent nearly 400,000 messages and posted 890,000 comments from 320,000 "hijacked" MySpace.com user accounts. (Id. ¶ 7, 13.) Defendant also created "groups" on MySpace.com redirecting users to the Wallace Websites, including altering the MySpace "unsubscribe" link to point to the Wallace Websites rather than to actually allow members to unsubscribe, and he used software code to lay graphics containing links to the Wallace Websites over users' MySpace.com profiles. (Id. ¶ 11-12.)

Plaintiff claims it has been harmed by Defendant's activity, including incurring bandwidth and delivery-related costs, costs associated with devoting time, money, and resources to stop Defendant's activities, and harm to its reputation from 800 complaints lodged by users over Defendant's activities. (Kaleel Decl. ¶¶ 20-21; Frazier Decl. ¶ 15.) The Wallace Websites also contain adult material, and since Plaintiff allows users as young as fourteen years old to create profiles, Defendant's activities on MySpace.com create the possibility that minors might view this offensive content. (Frazier Decl. ¶ 8, Exh. G; Kaleel Decl. ¶ 14.)

II. LEGAL STANDARD FOR A PRELIMINARY INJUNCTION

To obtain a preliminary injunction, a plaintiff must show "either: (1) a likelihood of success on the merits and the possibility of irreparable injury; or (2) that serious questions going to the merits were raised and the balance of hardships tips sharply in its favor." Walczak v. EPL Prolong, Inc., 198 F.3d 725, 731 (9th Cir. 1999). "These two alternatives represent extremes of a single continuum, rather than two separate tests." Id. (internal quotations omitted). "Thus, the greater the relative hardship to [a plaintiff], the less probability of success must be shown." Id.; see also International Jensen, Inc. v. Metrosound U.S.A., Inc., 4 F.3d 819, 822 (9th Cir. 1993). Moreover, "[t]he district court must also consider whether the public interest favors issuance of the injunction." Southwest Voter Registration Educ. Project v. Shelley, 344 F.3d 914, 917 (9th Cir. 2003). A preliminary injunction is an "extraordinary remedy" for which the need must be "clear and unequivocal." Shelton v. National Collegiate Athletic Ass'n, 539 F.2d 1197, 1199 (9th Cir. 1976).

III. EVIDENTIARY OBJECTIONS

Plaintiff has objected to the entire declaration of Defendant's purported expert, Dr. Lawrence H. Miller. Miller's declaration purports to give legal conclusions on the interpretation of the statutes at issue in the Complaint, which is an impermissible subject for expert testimony. See Crow Tribe of Indians v. Racicot, 87 F.3d 1039, 1045 (9th Cir. 1996) ("Expert testimony is not proper for issues of law."); Mukhtar v. California State Univ., Hayward, 299 F.3d 1053, 1066 n.10 (9th Cir. 2002) ("[A]n expert witness cannot give an opinion

as to her *legal conclusion, i.e.*, an opinion on an ultimate issue of law." (emphasis in original)). Moreover, Miller has not testified to any foundational knowledge of how MySpace.com works, and even mistakenly opines that MySpace.com users can only send messages to users on their "friends" list, which Plaintiff has persuasively demonstrated is simply incorrect. (Declaration of Aber Whitcomb ("Whitcomb Decl.") ¶ 8.) Finally, Miller is qualified only to testify as an engineer at an aerospace corporation, and yet he offers opinions on advertising issues, consumer perceptions, and social networking sites such as MySpace.com, areas in which he has no apparent qualifications. His testimony on these points is not reliable as required by Kumho Tire Co. v. Carmichael, 526 U.S. 137, 149 (1999). Therefore, the Court sustains Plaintiff's objections to the Miller Declaration and will accord his testimony no weight.

The Court has also reviewed and considered all other evidentiary objections to facts on which the Court has relied, and hereby overrules those objections.

III. ANALYSIS

Plaintiff seeks a preliminary injunction based on violations of the CAN-SPAM Act, 15 U.S.C. §§ 7704(a)(1), (a)(3), (a)(5) and (b)(2), and violations of Cal. Bus. & Prof. Code § 17529.5,§§ 22984 et seq., §§ 17200 et seq., and §§ 17500 et seq. As discussed below, the Court finds that Plaintiff has demonstrated a likelihood of prevailing on the merits of its claims under section 7704(a), so the Court need not determine whether Plaintiff will also prevail on its state-law claims.

A. Likelihood of Success on the Merits.

The CAN-SPAM Act, 15 U.S.C. §§ 7701 et seq. (the "Act"),

regulates the manner in which commercial email is transmitted and regulates various activities related to commercial email, such as prohibiting the use of false, misleading, or deceptive information, prohibiting the use of automated "bots" to create multiple email accounts, and requiring certain contact information in commercial electronic mail messages. 15 U.S.C. § 7704(a)(1), (a)(3), (a)(5), (b)(2). An "Internet access service" provider may seek to enjoin conduct prohibited by sections 7704(a)(1) and 7704(b), or enjoin a "pattern or practice" that violates section 7704(a)(2)-(5) and may seek either actual or statutory damages, whichever is greater. Id. § 7706(g)(1), (3). However, because section 7704 is limited to regulating only "commercial electronic mail messages," Plaintiff's private right of enforcement exists only if Defendant's messages fall within this statutory definition.

In opposition to Plaintiff's claims under the Act, Defendant first argues that messages sent from MySpace.com member accounts do not qualify as "electronic mail messages" as defined in the Act, and therefore, Defendant cannot be liable under any of the Act's provisions. The Act defines an "electronic mail message" as "a message sent to a unique electronic mail address." Id. § 7702(6). An "electronic mail address" is "a destination, commonly expressed as a string of characters, consisting of a unique user name or mailbox (commonly referred to as the 'local part') and a reference to an Internet domain (commonly referred to as the 'domain part'), whether or not displayed, to which an electronic mail message can be sent or delivered." Id. §7702(5). A "domain name" is "any alphanumeric designation which is registered with or assigned by any domain name

registrar, domain name registry, or other domain name registration authority as part of an electronic address on the Internet." Id. § 7702(4).

Defendant argues that MySpace.com messages do not fall within the Act's definitions of "electronic mail message" and "electronic mail address" because the addresses to which those messages are sent lack a "domain name" and have no route, instead remaining within the MySpace.com system. The Court rejects these contentions. The Court must assume that Congress expressed the legislative purpose of a statute through the ordinary meaning of the words used. See Leisoni, Inc. v. Stratman, 154 F.3d 1062, 1066 (9th Cir. 1998). The plain language of the definition of "electronic mail address" entails nothing more specific than "a destination . . . to which an electronic mail message can be sent," and the references to "local part" and "domain part" and all other descriptors set off in the statute by commas represent only one possible way in which a "destination" can be expressed. Indeed, the word "commonly" precedes the description of an address with a domain part and local part, indicating that this formulation is only one among many possible examples, rather than the exclusive way in which the Act recognizes the expression of an address. As Defendant himself points out, at the time the Act was passed in 2003, electronic messages could be sent in many ways, including through "instant messaging," and the Court must presume that Congress was well-aware of these various forms of electronic communications when it drafted the Act. The plain language of "electronic mail address" encompasses these alternate forms while also recognizing that the most commonly used form of electronic address was

the traditional "email" address with a local part and domain part (i.e., "user@domain.com"). This expansive interpretation of the Act supports the stated purpose of the Act, namely, curtailing the rapid and detrimental growth of commercial electronic mail that has overburdened electronic mail systems. 15 U.S.C. § 7701(a); see MySpace, Inc. V. The Globe.com, Inc., Case No. 06-3391, 2007 WL 1514783, *4 (C.D. Cal. February 27, 2007) ("[T]he overarching intent of this legislation is to safeguard the convenience and efficiency of the electronic messaging system, and to curtail overburdening of the system's infrastructure."). To interpret the Act in the limited manner as advocated by Defendant would conflict with the express language of the Act and would undercut the purpose for which it was passed.

Even under Defendant's more restrictive interpretation, however, messages sent through MySpace.com fall within the definition of "electronic mail message" sent to an "electronic mail address." Each MySpace.com user's mail resides on a unique URL, which includes a string of characters containing the member's username and a reference to the domain "myspace.com." (Whitcomb Decl. ¶ 4.) MySpace.com messages also contain header information, such as source, destination, and routing information, and references to the unique username and the myspace.com domain name. (Id. ¶ 5.) As the court in MySpace, Inc. aptly stated in response to this precise argument, "[w]hile the routing employed by MySpace may be less complex and elongated than those employed by traditional [Internet service providers], *any* routing necessarily implicates issues regarding volume of traffic and utilization of infrastructure -- issues which CAN-SPAM seeks to

address." 2007 WL at *5. Therefore, even under Defendant's unduly narrow interpretation, each MySpace.com message qualifies as an "electronic mail message" sent to an "electronic mail address." Plaintiffs may properly bring suit under the Act against Defendant.

a. § 7704(a)(1)

Section 7704(a)(1) prohibits the use of false or misleading header information, including header information that is "technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations." 15 U.S.C. § 7704(a)(1)(A). "Header information" is defined as "the source, destination, and routing information attached to an electronic mail message, including the originating domain name and originating electronic mail address, and any other information that appears in the line identifying, or purporting to identify, a person initiating the message." Id. § 7702(8). Plaintiff need not demonstrate a "pattern or practice" to bring a claim under this subsection. Id. § 7706(g)(1).

Plaintiff argues that Defendant violated this subsection by obtaining 342,000 MySpace.com members' usernames and passwords through the Wallace Websites that misleadingly and falsely resembled the log-in page at MySpace.com. He then used this information to log into those members' accounts and send 400,000 spam messages from those accounts to other users. Plaintiff also argues that Defendant falsely obtained over 11,000 "dummy" MySpace.com profiles to spam other members, collect members' personal information, send commercial messages, and post prohibited content, all in violation of the TOU

Contract. Defendant claims that these allegations do not relate to "headers" as required by this subsection, and even if they did, the header information could not be altered or faked, so all the header information was accurate. Further, Defendant argues that a MySpace.com member cannot "arbitrarily" send out messages, but rather each recipient must be on that member's "friends" list, making it impossible for Defendant to violate this subsection.

Defendant is correct that, whatever the means by which he created 11,000 MySpace.com profiles, this activity, in itself, did not involve sending messages with header information and does not implicate section 7704(a)(1). The 400,000 messages Defendant sent via 340,000 other members' profiles, however, clearly violated this subsection. In section 7704(a)(1)(A), Congress intended to prohibit not only sending messages with inaccurate header information, but also sending messages with accurate header information, access to which was obtained through false or fraudulent pretenses. See Sen. Rep. No. 108-102 at 17 (2003) (stating that one purpose of section 7704(a)(1)(A) "is to eliminate the use of inaccurate originating email addresses that disguise the identities of the senders."). Here, Defendant obtained access to other members' usernames and passwords by creating websites that appeared nearly identical to the log-in page at MySpace.com. (Frazier Decl. ¶¶ 7-8, Exh. E.) He then used that information to "hijack" 340,000 member accounts to send out mass commercial messages. This clearly falls within the category of messages prohibited where the header might be accurate but access to the account from which it came was falsely and fraudulently obtained. That messages could not be sent "arbitrarily" is irrelevant (and an

inaccurate factual statement as discussed above) -- nothing in this subsection requires that messages must be sent "arbitrarily" and reading such a requirement into the statute would seriously undermine the efficacy of this subsection. Therefore, Plaintiff has demonstrated a likelihood of success on its claim under section 7704(a)(1).

b. § 7704(a)(3)

Section 7704(a)(3) prohibits sending commercial electronic mail that does not contain a functioning return electronic mail address, active for at least 30 days following the date of the message, to which a recipient can send a request that no further messages be sent. 15 U.S.C. § 7704(a)(3)(A). To bring a private cause of action under this subsection, Plaintiff must demonstrate a "pattern or practice" of prohibited conduct. Id. § 7706(g)(1). Plaintiff argues that Defendant violated this provision by sending messages from other users' accounts, so that any reply message sent by a user to decline further messages would go to the unwitting sender, not to Defendant. Defendant argues that a recipient can, in fact, reply to a message sent from another user because the messages contain information on the sender and the sender must be on the recipient's "friends" list to send the message in the first place.

Defendant again ignores the plain language of the Act. The subsection requires that messages contain a functioning return electronic mail address to which a recipient can respond to request no further messages. Defendant's use of "hijacked" profiles to send messages from a user other than Defendant completely eviscerates a recipient's ability to request no further messages from the actual

spammer. Any request to stop sending messages would not go to the individual responsible for the spam message, but rather, to an unwitting sender who cannot control Defendant's surreptitious use of their account. Congress clearly intended this provision to enable recipients of commercial spam to contact the spammer to curb further spamming. Interpreting it as advocated by Defendant would undercut this purpose and encourage "hijacking" as an end-run around this subsection.

Plaintiff asserts that Defendant's prohibited conduct under this subsection amounted to a "pattern or practice" of violations and Defendant makes no argument specifically refuting this contention. The terms "pattern or practice" are undefined in the Act, but in other contexts, the Ninth Circuit has stated that "these terms have their ordinary meaning." Cherosky v. Henderson, 330 F.3d 1243, 1246-47 (9th Cir. 2003); see also United States v. Ironworkers Local 86, 443 F.2d 544, 552 (9th Cir. 1971) ("The words [pattern or practice] were not intended to be words of art."). One isolated act in violation of the Act is insufficient. See Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 358 (4th Cir. 2006) (granting summary judgment on section 7704(a)(3) claim because one violation did not demonstrate a pattern or practice). The evidence indicates that, beginning as early as October 2006, Defendant began his activities to obtain MySpace.com members' log-in information and to send out unsolicited emails. (Frazier Decl. ¶¶ 2-3.) Specifically, Plaintiffs offered evidence of at least three separate "attacks" by Defendant using other members' profiles to send commercial messages:

- On March 27, 2007, Plaintiff's abuse team discovered that

Defendant used 328,303 profiles to send 392,726 unsolicited messages. (Id. ¶ 7.)

- On May 16, 2007, the abuse team discovered that Defendant used at least 5,306 user profiles to send 5,783 unsolicited messages. (Id. ¶ 9.)
- On May 20, 2007, the abuse team discovered that Defendant used 8,935 user profiles to send at least 10,125 unsolicited messages. (Id. ¶ 8.)
- Since Plaintiff filed its motion, the abuse team has discovered an additional 110,000 messages sent from 76,200 user accounts between May 10, 2007 and June 14, 2007. (Kaleel Supp. Decl. ¶ 11.)

This detailed record adequately demonstrates that Defendant has engaged in a pattern of violations sufficient under section 7706(g)(1) to support Plaintiff's private cause of action. Therefore, Plaintiff has demonstrated a likelihood of succeeding on its section 7704(a)(3) claim.

c. § 7704(a)(5)

Section 7704(a)(5) requires that all commercial electronic messages contain "clear and conspicuous identification that the message is an advertisement or solicitation," "clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender," and "a valid physical postal address of the sender." 15 U.S.C. § 7704(a)(5)(A). This provision also requires Plaintiff to demonstrate a pattern or practice of violations. Id. § 7706(g)(1).

Plaintiff claims that Defendant violated this provision with 400,000 messages that did not identify themselves as advertisements, did not contain notice of an opportunity to opt out of receiving further messages, and did not contain a physical address for Defendant. Plaintiff also argues that this information was absent

from messages sent from users' hijacked accounts. Defendant argues that the messages were not "commercial," but rather invitations to view pictures, e-cards, or other non-commercial material, and even so, the messages contained a MySpace.com return address.

The Act defines "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." 15 U.S.C. § 7702(2)(A). Regulations passed under the Act further define the term "primary purpose" as "an electronic mail message [that] consists exclusively of the commercial advertisement or promotion of a commercial product or service[.]" 16 C.F.R 316.3(a)(1). The plain language of this subsection indicates that "commercial electronic mail messages" include messages that may not themselves appear commercial, but that promote a "commercial service" such as an "Internet website operated for a commercial purpose." 15 U.S.C. § 7704(a)(5)(A). Although the Wallace Websites do not appear to request any money directly from visitors and Defendant created the websites to "provide fun, viral websites designed to motivate Internet user[s] to refer their friends to view the content, sometimes called a 'tell-a-friend' service," (Wallace Decl. ¶ 3, Exh. C.), Defendant admits that his "Internet business" earns him approximately $1 million per year (Id. ¶ 15). The record is silent as to how Defendant specifically earns this revenue, but evidence on this point is unnecessary. The Court can readily infer that Defendant operates the Wallace Websites, his "Internet business," to generate his $1 million a year in revenue, and the facts demonstrate that he sent hundreds of

thousands of messages directing recipients to these websites. Therefore, these messages, even if not commercial on their face, promote an "Internet website operated for a commercial purpose" and are "commercial electronic mail messages" subject to the Act.

Defendant does not dispute that the messages did not contain "clear and conspicuous identification that the message is an advertisement or solicitation," "clear and conspicuous notice of the opportunity to decline to receive further commercial electronic mail messages from the sender," and "a valid physical postal address of the sender." Further, even if the messages Defendant sent from "hijacked" accounts contained a return address, that address would be wholly ineffective to allow the recipient to "opt out" of receiving further messages since Defendant -- the one engaging in the commercial solicitation -- would never receive those requests. Finally, as discussed above, the evidence submitted by Plaintiff demonstrates a pattern of acts that violate this subsection. Therefore, Plaintiff has demonstrated a likelihood of success on the merits of its claim under section 7704(a)(5).

d. Section 7704(b)(2)

Section 7704(b)(2) prohibits a person from using "scripts or other automated means to register for multiple electronic mail accounts or online user accounts from which to transmit . . . a commercial electronic mail message that is unlawful under subsection (a)" of section 7704. 15 U.S.C. § 7704(b)(2). Showing a pattern or practice under this provision is unnecessary to maintain a private cause of action. Id. § 7706(g)(1). Plaintiff argues that the Court should infer a violation of this section because the naming

conventions used in creating 11,000 separate profiles were consistent, including 2,077 profiles named "What Pic Should I Upload?", as were the naming conventions in the underlying America Online email addresses. (Kaleel Decl. ¶¶ 16-18.) Defendant argues that Plaintiff has presented no evidence that he used a "bot" to register these profiles and in any event, each registration requires the user to input a unique set of characters designed to be unreadable to an automated program, and Plaintiff has not offered any evidence on how such an automated script could be written.

Plaintiff need not necessarily provide direct evidence that Defendant used an automated bot for registration, but it must provide evidence sufficient for the Court to infer such use, and Plaintiff has failed to do so. Plaintiff's only evidence is the creation of 11,000 profiles, 2,000 of which share the same name, and all of which were registered using similar America Online email addresses. These facts do not necessarily compel the conclusion that Defendant used an automated bot. For example, Plaintiff has not provided evidence of the time frame in which the 11,000 profiles were created, which is crucial because, assuming registration of a new profile takes only one minute (which is conservative given that the user must input a name, country, zip code, birth date, gender, an email address, and a unique verification code, as well as create a password and agree to the TOU Contract), one person could spend 23 eight-hour days, without breaks, to create 11,000 profiles. While this may seem unrealistic, Defendant could also have hired others to assist in this registration process, substantially reducing the time and effort needed from a single person. On the other hand, evidence that the registration of the

11,000 profiles occurred over a matter of hours or even days would greatly strengthen any inference that the registration was done with an automated bot.

Moreover, Plaintiff has provided no evidence that an automated bot could circumvent the verification step in the registration process, a security measure used by Plaintiff to stop automated registration. Plaintiff suggests instead that Defendant could have used an automated bot to complete all steps up to the verification code step. While this may be true, and the Court certainly would not require Plaintiff to disclose trade secrets or outline the specific steps to circumvent its security measures to prove this point, the record is devoid of any testimony that this type of automated bot exists or has been used in the past. Defendant, on the other hand, testified that he has no knowledge of any automated script that could circumvent this security measure. (Wallace Decl. ¶ 9.) The Court recognizes that at the preliminary stage the evidentiary burden is relaxed, see Flynt Distrib. Co. v. Harvey, 734 F.2d 1389, 1394 (9th Cir. 1984), but the evidence in the record at this time is simply insufficient to demonstrate that Plaintiff will likely prevail on the merits of its claim under this subsection.

B. Irreparable Harm

Plaintiff claims it has been irreparably harmed by Defendant's activities because Defendant's messages have clogged the MySpace.com network, used up bandwidth, and degraded the user experience. (Kaleel Decl. ¶¶ 11-12.) This has resulted in delivery-related costs, and costs associated with devoting time, money, and resources to stop Defendant's activities. (Kaleel Decl. ¶ 21.) Moreover, Plaintiff's

reputation and business goodwill have suffered, manifested by 800 complaints lodged by users over Defendant's activities. (Frazier Decl. ¶ 15.)[2]

Harm to business goodwill and reputation is unquantifiable and considered irreparable. See Rent-A-Center, Inc. v. Canyon Tele. & Appliance Rental, Inc., 944 F.2d 597, 603 (9th Cir. 1991) ("Intangible injuries, such as damage to ongoing recruitment efforts and goodwill, qualify as irreparable harm."); Optinrealbig.com, LLC v. Ironport Sys., Inc., 323 F. Supp. 2d 1037, 1050 (N.D. Cal. 2004) ("Damage to a business's goodwill is typically irreparable injury because it is difficult to calculate."). Plaintiff has incurred substantial costs in detecting, investigating, and remedying Defendant's unsolicited messages, including removing over 290,000 unauthorized links and over 890,000 comments throughout the MySpace.com site. (Frazier Decl. ¶¶ 13-14.) Moreover, Plaintiff has received 800 complaints about Defendant from users. While that may only amount to one complaint for every thousand unsolicited messages, this is still a substantial number and constitutes injury to Plaintiff's goodwill. (Kaleel Supp. Decl. ¶ 8); see Compuserve Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (finding that Defendant Wallace inflicted harm to plaintiff's business reputation and goodwill by causing subscribers to terminate their accounts). Further, the Court

---

[2]Plaintiff also argues that, since users as young as fourteen years old can create profiles on MySpace.com, Defendant's activities create the risk that minors using MySpace.com might view adult material contained on the Wallace Websites. (Frazier Decl. ¶ 8, Exh. G; Kaleel Decl. ¶ 14.) Defendant disputes this contention. The Court need not address this point since Plaintiff sufficiently demonstrated irreparable harm through the other evidence it has submitted.

cannot expect every user to complain about every piece of spam received, since users would spend as much time responding to spam as they would responding to non-spam messages. See 15 U.S.C. § 7701(2) ("Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic . . ."). Moreover, Defendant's misleading suggestions that he is affiliated with Plaintiff impacts the quality of MySpace.com users' experiences with Plaintiff's services. See Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q.2d 1020, 1025-26 (N.D. Cal. 1998) (finding irreparable harm where defendants caused customer confusion by suggesting they were associated with plaintiff); Meineke Car Care Centers, Inc. v. Quinones, 2006 WL 1549708, *3 (W.D.N.C. 2006) (finding that lost customers resulting from defendants' deceptive suggestion that they were associated with plaintiff constituted irreparable harm).[3] For these reasons, Plaintiff has persuasively demonstrated irreparable harm from Defendant's unlawful activities.

C. Balance of Hardships and Public Interest

The balance of hardships tips sharply in favor of Plaintiff here. Plaintiff has already expended substantial time and money in combating Defendant's unsolicited messages and postings, and has dealt with over 800 resulting user complaints. Moreover, Plaintiff has discovered

---

[3]Defendant distinguishes Hotmail Corp. on the ground that it involved a claim for trademark infringement. Although that is true, the irreparable harm inquiry is not dependent on the claims asserted, but rather the harm suffered as a result of the defendant's allegedly unlawful actions. Here, Defendant caused confusion by using the MySpace.com logo and log-in box to deceive users into providing their log-in information. This activity creates the same risk of harm as in Hotmail Corp. -- the potential loss of customers -- and therefore the court's analysis in that case is equally applicable here.

further evidence that Defendant's actions have continued even after Plaintiff filed the instant motion, discovering yet another group of 110,000 messages sent from 76,200 user accounts between May 10, 2007 and June 14, 2007. (Kaleel Supp. Decl. ¶ 11.) Plaintiff also suggests that, short of an injunction, it would experience difficulty in curbing Defendant's activities by, for example, blocking Defendant's Internet Protocol addresses, without also curbing other users' legitimate use. (Kaleel Supp. Decl. ¶ 5.) Even if it blocked his IP addresses, he could modify his equipment and tactics to circumvent this security measure. See, e.g., Compuserve Inc., 962 F. Supp. at 1019 (stating that, in response to software programs blocking Defendant Wallace and his company's messages, they "have modified their equipment and the messages they send in such a fashion as to circumvent Compuserve's screening software."). In contrast, as outlined above, Defendant's actions likely violate the CAN-SPAM Act and he would experience no hardship if enjoined from committing any further violations. See Phillip Morris USA Inc. v. Shalabi, 352 F. Supp. 2d 1067, 1075 (C.D. Cal. 2004).

The public interest is also served through enjoining Defendant's unlawful activities. In passing the CAN-SPAM Act, Congress recognized the significant costs and burden associated with the nearly unchecked growth of commercial spam. 15 U.S.C. § 7701. "[B]arraging the public with spam" injures the public such that the public "is forced to incur the costs of needlessly expended energy and time evaluating and eventually discarding defendants' unsolicited messages[.]" F.T.C. v. Phoenix Avatar, LLC, 2004 WL 1746698, *14 (N.D. Ill. 2004) (enjoining violations of the CAN-SPAM Act). Because Defendant's activities fall

squarely within those activities Congress found detrimental to the public in the CAN-SPAM Act, this factor strongly weighs in favor of Plaintiff.

IV. SCOPE OF INJUNCTION

Defendant challenges Plaintiff's proposed injunction as too broad, sweeping in Defendant's legitimate activities along with any alleged unlawful ones. Plaintiff's proposed injunction seeks to enjoin Defendant from the following:

> (a) "accessing or using the MySpace.com website, MySpace Internet messaging service and/or any other services offered by or through MySpace (the 'MySpace Service') to directly or indirectly send or transmit any electronic communications, emails or instant messages to any MySpace user or MySpace account or to post comments or bulletins";
>
> (b) "establishing or maintaining MySpace profiles or accounts";
>
> (c) "using the MySpace Service for a commercial purpose";
>
> (d) "referring in any way to MySpace in connection with any unsolicited commercial electronic communication, email or instant message";
>
> (e) "using any automated scripts, bots, or other executable programs in connection with any MySpace account or the MySpace service or providing such programs to third parties for use on the MySpace Service";
>
> (f) "soliciting, requesting, or taking any action to induce a MySpace user to provide identifying information, including MySpace account information such as a username and/or password"; and
>
> (g) "using another MySpace user's identifying information, including MySpace account information such as username and/or password";
>
> (h) "referencing MySpace in connection with any advertisements []"; and
>
> (i) "[encouraging], facilitating, enabling or inducing any person or entity to do any of the above in violation of the CAN SPAM Act, 15 U.S.C. § 7701 et seq. and California Business & Professions Code §§ 17529.5, 17200 et seq., 17500 et seq., and 22948."

Defendant argues that subsections (d) and (h) sweep in legitimate commercial speech in violation of his First Amendment rights. Plaintiff refutes this claim by citing two cases to suggest that courts have rejected Defendant's First Amendment arguments in similar circumstances. See Cyber Promotions v. America Online, Inc., 948 F. Supp. 436, 455 n.7 (E.D. Pa. 1996); Compuserve, 962 F. Supp. at 1024. Plaintiff, however, misinterprets the opinions in both America Online and Compuserve. In America Online, the court specifically limited its discussion to activities on the America Online site, not on the Internet, stating that "AOL has never sought to control the exchange of ideas and communications over the Internet itself. Rather, AOL has sought to control its own pathway or channel leading to the Internet in order [to] protect its own private property, reputation and subscribers from Cyber's mass email advertisements." 948 F. Supp. at 454-455. Similarly, in Compuserve, the court's analysis centered on "Defendant's use of plaintiff's proprietary computer equipment," not on regulating the channels of speech on the greater Internet. 962 F. Supp. at 1027.

The Court finds that subsections (d) and (h) are, in fact, too broad, risking infringement of Defendant's legitimate commercial and non-commercial speech activities outside Plaintiff's proprietary MySpace.com site and beyond the limitations upheld in America Online and Compuserve. Defendant has a legitimate First Amendment right to mention Plaintiff, even in commercial solicitation messages, so long as recipients are not misled into believing that Defendant is somehow associated with or speaking for Plaintiff. For example, Defendant has the right, in any commercial message, to engage in critical discussion

of Plaintiff, Plaintiff's lawsuit against him, or to truthfully discourage recipients from utilizing Plaintiff's services. As both subsections (d) and (h) are currently drafted, Defendant could not engage in this speech and enjoining Defendant consistent with these provisions would, in fact, violate Defendant's free speech rights.

Subsections (f) and (g) also risk curbing the legitimate activities of third parties. As they are drafted, subsections (f) and (g) would preclude Defendant from obtaining fully informed, knowing, and voluntary consent from MySpace.com members so that Defendant might log on to their accounts and disseminate messages (commercial or otherwise). Although the record does not reflect that any member has (or would) consent to such a use of his or her account, this possibility exists and the Court cannot enjoin this legitimate choice by members, so long as Defendant fully informs them that he is not affiliated with or sanctioned by Plaintiff, and that he intends to use that information to log in to their MySpace.com accounts and disseminate messages to other MySpace.com users. Therefore, subsections (f) and (g) are too broad.

Further, the Court cannot enjoin Defendant based on subsection (e) because, as discussed above, the Court finds that Plaintiff has not demonstrated a likelihood of success on the merits of its section 7704(b)(2) claim. The Court notes that omitting this subsection of the proposed injunction on this basis may have little practical effect since subsection (b) prevents Defendant from establishing MySpace.com accounts or profiles by any means, including through automated bots.

The remaining provisions (a), (b), and (c) relate specifically to Defendant's use of Plaintiff's space, equipment, and property. As

Plaintiff points out, MySpace.com is a private site, the use of which is a privilege, and Defendant has repeatedly demonstrated his inability to comply with Plaintiff's rules of use or with federal law when using Plaintiff's services. Therefore, these provisions validly prevent Defendant from abusing the privilege of using Plaintiff's services and are adequate in scope to fulfill this purpose.[4]

V. BOND

Federal Rule of Civil Procedure 65(c) requires Plaintiff to post a bond, in a sum the Court deems appropriate, for the payment of costs and damages that Defendant may suffer if he is later found to have been wrongfully enjoined. While the Court recognizes that a bond may not be required when the harm to the enjoined party is minimal, see, e.g., Jorgensen v. Cassiday, 320 F.3d 906, 919 (9th Cir. 2003), the Court retains discretion to require a bond when the party seeking the injunction has not offered evidence of its own harm in posting a bond, see Barahona-Gomez v. Reno, 167 F.3d 1228, 1237 (9th Cir. 1999). Plaintiff has argued only that an injunction would impose no hardship on Defendant, not that Plaintiff itself will suffer some harm in posting a bond. Plaintiff requests a bond of $1 million, but the Court finds that a bond for this amount is unnecessary. Therefore, the Court ORDERS Plaintiff to post a bond in the amount of $50,000.

VI. CONCLUSION

Plaintiff has demonstrated a likelihood of success on the merits

---

[4]The Court notes that subsection (i) is necessary to the extent that it enjoins Defendant from directing others to undertake activities that he is prohibited from undertaking, although referring to the specific statutory provisions at issue is unnecessary because the other parts of the injunction clearly delineate the prohibited conduct.

of its claims under the CAN-SPAM Act, 15 U.S.C. § 7704(a)(1), (a)(3), and (a)(5), but has not offered sufficient evidence to demonstrate a violation of section 7704(b)(2). Plaintiff has also demonstrated irreparable harm to its business goodwill and reputation if Defendant continues his unlawful activities, the balance of hardships tips in its favor, and the public interest is served by enjoining Defendant's conduct.

Therefore, the Court ENJOINS Defendant, his agents, servants, employees, representatives, and all other persons or entities acting on his behalf or in concert or participation with him, from[5]:

> (1) accessing or using the MySpace.com website, MySpace Internet messaging service and/or any other services offered by or through MySpace (the 'MySpace Service') to directly or indirectly send or transmit any electronic communications, emails or instant messages to any MySpace user or MySpace account or to post comments or bulletins;
>
> (2) establishing or maintaining MySpace profiles or accounts;
>
> (3) using the MySpace Service for a commercial purpose;
>
> (4) referring to MySpace in connection with any unsolicited commercial electronic communication, email or instant message, in any way that falsely or fraudulently suggests that such message was approved by, generated by, or is in any way affiliated with MySpace;
>
> (5) using any MySpace logo or using any graphic, interface, or other presentation that approximates or resembles the MySpace.com log-in page to mislead users into believing that they are logging onto their MySpace.com accounts rather than providing Defendant with their username and password;
>
> (6) inducing a MySpace user to provide MySpace identifying information, including MySpace account information such as a username and/or password, without first informing the user the Defendant is not affiliated with or sanctioned by MySpace and without obtaining fully informed, knowing, and voluntary consent through a separate affirmative step by the

---

[5]These provisions incorporate a combination of Plaintiff's proposed provisions and the Court's limitations as outlined supra.

user; and

(7) encouraging, facilitating, enabling or inducing any person or entity to do any of the above.

Plaintiff is ORDERED to post a bond in the amount of $50,000 **within ten (10) days of the date of this Order.** Plaintiff is also ORDERED to prepare a proposed order consistent with this Order, including findings of fact and conclusions of law, **within ten (10) days of the date of this Order.**

IT IS SO ORDERED.

DATED: July 2, 2007

AUDREY B. COLLINS
UNITED STATES DISTRICT JUDGE